UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

KATIE FULLER, individually and on behalf of all others similarly situated,

Plaintiff,

v.

LIFETIME HEALTHCARE, INC., d/b/a THE LIFETIME HEALTHCARE COMPANIES, and EXCELLUS HEALTH PLAN, INC., d/b/a EXCELLUS BLUECROSS BLUESHIELD,

Defendants.

Civil Action No. _____

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Katie Fuller ("Plaintiff"), by and through her attorneys, makes the following allegations pursuant to the investigation of her counsel and based upon information and belief, except as to allegations specifically pertaining to herself and her counsel, which are based on personal knowledge, against defendants Lifetime Healthcare, Inc., d/b/a The Lifetime Healthcare Companies ("Lifetime Healthcare"), and Excellus Health Plan, Inc., d/b/a Excellus BlueCross BlueShield ("Excellus," together with Lifetime Healthcare, "Defendants").

NATURE OF THE ACTION

1. On September 9, 2015, Excellus, one of the largest health insurance companies in New York State, announced a security breach (the "Data Breach") that exposed the personally identifiable information of approximately 10 million customers.

2. According to Excellus, the Data Breach began as long ago as December 23, 2013. Thus, by Defendants' own account, it took nearly two years for Excellus to detect the breach and inform customers.

3. The wrongfully disclosed information includes extremely sensitive and vital personal information, including, but not limited to, customers' names, dates of birth, social

security numbers, addresses, telephone numbers, member identification numbers, financial information, and medical claims information ("Personal Information").

4. The Excellus breach is just one of several data security breaches involving a health care company affiliated with BlueCross BlueShield, including the earlier Anthem, Premera, and CareFirst breaches. Defendants knew Excellus was a potential target of data theft and cyber intrusion and knew the importance of keeping customers' Personal Information safe from cyber criminals.

5. Defendants had a duty to put in place and maintain adequate security measures to safeguard the Personal Information that Plaintiff and other members of the Class (as defined herein) entrusted to it.

6. Because Defendants failed to take necessary precautions to safeguard Class members' information, Class members' Personal Information was and may remain available for illegal misuse for years.

7. As a direct and proximate result of Defendants' wrongful actions, inaction, and omissions, and the resulting Data Breach, Class members have suffered and will continue to suffer economic damages, including *inter alia* the costs of monitoring their credit, monitoring their financial accounts, and mitigating their damages, and they face an immediate and substantial risk of identity theft and fraud, as well as damage to their credit score.

8. Plaintiff brings this action, on behalf of herself and all others similarly situated, against Defendants for failing to safeguard her and other Class members' Personal Information, and for failing to provide timely and adequate notice to Plaintiff and other Class members that their information had been stolen and of the scope and the extent of the breach. Plaintiff asserts claims for negligence, negligence per se, breach of implied contract, bailment,

conversion, unjust enrichment, and violations of New York General Business Law § 349. Plaintiff seeks damages, restitution, and injunctive relief on behalf of the Class.

PARTIES

9. Plaintiff is a citizen of the state of New York, residing in Clinton County, New York. Plaintiff is a former Excellus customer. In October or November, 2015, Plaintiff received notification letters from Excellus, notifying her that the Personal Information of herself and her three children had been compromised and exposed to thieves.

10. Defendant Lifetime Healthcare, Inc., d/b/a The Lifetime Healthcare Companies, is a New York not-for-profit corporation with its principle place of business at 165 Court Street, Rochester, New York 14647. Lifetime Healthcare operates a $6 billion group of companies that provide health care services and health insurance within New York and provide certain long-term care services nationwide.

11. Defendant Excellus Health Plan, Inc., d/b/a Excellus BlueCross BlueShield, is a New York not-for-profit corporation with its principle place of business at 165 Court Street, Rochester, New York 14647. Excellus is a subsidiary of Lifetime Healthcare and is an independent licensee of the Blue Cross Blue Shield Association.

JURISDICTION AND VENUE

12. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) because there are more than 100 Class members and the aggregate amount in controversy exceeds $5,000,000, exclusive of interest, fees, and costs, and at least one Class member is a citizen of a state different from Defendants.

13. This Court has personal jurisdiction over Defendants because Defendants are headquartered and incorporated in New York, and conduct substantial business within New

York, such that Defendants have significant, continuous, and pervasive contacts with the State of New York.

14. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendants are headquartered in this District, do substantial business in this District, caused harm to Class members in this District, and a substantial part of the events giving rise to Plaintiff's claims took place within this judicial district.

FACTUAL BACKGROUND

Excellus

15. Excellus is a health care company operating under Lifetime Healthcare—a $6.6 billion family of companies.

16. In 1996, Excellus was created by the merger of the BlueCross BlueShield Plans in Central New York and Rochester. In 1997, BlueCross BlueShield of Utica-Watertown joined Excellus and, in 2003, the BlueCross BlueShield Plans of Central New York, the Rochester Area, and Utica-Watertown became known as Excellus BlueCross BlueShield.

17. Excellus delivers health care services across upstate New York, including to 31 New York State counties, and long term care insurance nationwide. The company provides health insurance to approximately 1.6 million members, employs approximately 6,000 New Yorkers, and possesses the Personal Information of approximately 10 million individuals.

18. Excellus knows that the Personal Information it maintains is sensitive and of vital importance to its customers. Excellus is well aware that it has a legal obligation to protect this information. The Excellus website acknowledges, "Privacy laws prohibit us from disclosing protected health information (PHI) related to your health insurance coverage to another person or organization (with some exceptions, like your physician) without your

written authorization." https://www.excellusbcbs.com/wps/portal/xl/mbr/mgr/manageprivacy/ (last visited Nov. 25, 2015).

19. Excellus' privacy notice to customers explains Excellus' "commitment" to customers' privacy and states, *inter alia*:

> We understand that medical information about you and your health is personal. We are committed to safeguarding your protected health information (PHI). . . . The law requires us to:
>
> - make sure that PHI that identifies you is kept private;
> - give you this notice of our legal duties and privacy practices with respect to PHI about you; and
> - follow the terms of the notice that is currently in effect.

Excellus Privacy Policy, effective April 14, 2003, dated August 2013.

20. The privacy notice further acknowledges that Excellus is "required by applicable federal and state laws to maintain the privacy of your PHI" and notify customers in the event of "a breach of your unsecured PHI." It explains, "Nonpublic Personal Information is information you give us on your enrollment form, claim forms, premium payments etc. For example: names, member identification number, social security number, addresses, type of health care benefits, payment amounts, etc." Excellus assures customers it will not give out nonpublic personal information to anyone without customer consent and it advises customers that it employs safeguards, including, "a privacy oversight committee," "a security coordinator to detect and prevent security breaches," and "security protections" on "all computer systems that contain personal information."[1]

[1] *See also* https://www.excellusbcbs.com/wps/portal/xl/our/compliance/privacy ("At Excellus BlueCross BlueShield, we know how important your privacy is to you. Therefore, we are committed to protecting any personal information that you provide us on this website according to applicable laws, regulations and accreditation standards and practices, and we continue to evaluate new administrative, technical and physical safeguards for protecting your information.").

21. Although Defendants were well aware of their legal duty to protect Class members' Personal Information, they failed to honor these promises and violated their legal obligation to protect customer's Personal Information.

HIPAA

22. The Health Insurance Portability and Accountability Act ("HIPAA") sets national standards for the security of electronic health information, requirements for notification in the event of a breach, and requirements for the privacy of individually identifiable health information. *See* 45 C.F.R. § 164.

23. As a healthcare insurance provider, Excellus is required to protect its customers' Personal Information, including by adopting and implementing the specific data security standards set forth under HIPAA.

24. Under HIPAA, entities, including Excellus, must, *inter alia*, "[e]nsure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits" and must "[p]rotect against any reasonably anticipated threats or hazards to the security or integrity of such information." *See* 45 C.F.R. § 164.306.

25. To fulfill these obligations, covered entities or businesses must "[i]mplement policies and procedures to prevent, detect, contain, and correct security violations," including "[c]onduct[ing] an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate" and "[i]mplement[ing] procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracing reports." *See* 45 C.F.R. § 164.308(a).

26. Such policies and procedures must protect against both physical and technical access to information. *See* 45 C.F.R. §§ 164.310, 164.312. Technical safeguards include implementing "a mechanism to encrypt and decrypt electronic protected health information;" "hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information;" "procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed;" and "technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network." *See* 45 C.F.R. § 164.312.

27. Defendants failed to comply with these requirements.

The Risk Of A Data Security Attack Was Known To Defendants

28. On April 8, 2014, the Federal Bureau of Investigation, Cyber Division ("FBI"), issued a Private Industry Notification entitled, "Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain," stating in part:

> Cyber actors will likely increase cyber intrusions against health care systems . . . due to mandatory transition from paper to electronic health records (EHR), lax cybersecurity standards, and a higher financial payout for medical records in the black market....
>
> [T]he health care industry is not technically prepared to combat against cyber criminals' basic cyber intrusion tactics, techniques and procedures (TTPs), much less against more advanced persistent threats (APTs). The health care industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely.

29. As the FBI stated, a 2014 report by the SANS Institute indicated that "health care security strategies and practices are poorly protected and ill-equipped to handle new cyber threats exposing patient medical records, billing and payment organizations, and intellectual property." As further noted by the FBI, other organizations focusing on cyber security and

privacy, such as Ponemon Institute and EMC Corporation, had issued reports in 2013 indicating that a lack of preparedness on the part of health care organizations posed serious risks to customer data.

30. Nonetheless, many health care organizations have failed to take action and have spent significantly less to secure their data than do businesses in other industries. Indeed, well before Excellus' discovery of its Data Breach, health insurance companies such as Anthem, CareFirst, and Premera each previously announced breaches of their own data systems.

31. Despite these clear warnings, Excellus failed to take necessary steps to secure and protect the Personal Information of its customers, or even to detect the Data Breach until approximately 20 months after it began.

The Data Breach

32. On September 9, 2015, Excellus announced that hackers had accessed a database holding the Personal Information of approximately 10 million customers and employees, including the Personal Information of Plaintiff and members of the Class.

33. Experts estimate that this information could be worth up to $1,000 per person on the black market.

34. According to Excellus, the company became aware of the Data Breach on August 5, 2015. Although it had already been over one month since Excellus detected the breach, the company announced an internal deadline of November 9, 2015, to notify affected customers.

35. Moreover, according to Excellus, the Data Breach began as early as December 23, 2013. Thus, by Excellus' own account, it took nearly two years for Defendants to detect the breach and alert their customers.

36. Excellus created a webpage at www.excellusfacts.com, which stated in part:

> Safeguarding the privacy of your personal information is a top priority for us, and we make every effort to protect your information. Despite these efforts, Excellus…was targeted in a very sophisticated cyberattack. We recognize the frustration and concern that this news may cause, and we are making services available to protect you and your information moving forward….
>
> We worked closely with Mandiant, one of the world's leading cybersecurity firms, to conduct our investigation and to remediate the issues created by the attack on our IT systems. We are taking additional actions to strengthen and enhance the security of our IT systems moving forward.
>
> Our investigation determined that the **attackers may have gained unauthorized access to individuals' information, which could include name, date of birth, Social Security number, mailing address, telephone number, member identification number, financial account information and [medical] claims information. This incident also affected members of other Blue Cross Blue Shield plans who sought treatment in the 31 county upstate New York service area of Excellus BCBS. Individuals who do business with us and provided us with their financial account information or Social Security number are also affected.** …
>
> …We are providing **two years of free identity theft protection services through Kroll**, a global leader in risk mitigation and response solutions, **including credit monitoring powered by TransUnion**, to affected individuals. We also have established a dedicated call center for affected individuals to contact with any questions….

(Emphasis added.)

37. Plaintiff and Class members entrusted Defendants with their Personal Information and Defendants had a duty to protect and secure the Personal Information entrusted to them. Defendants betrayed Plaintiff's and Class members' trust by failing to properly safeguard and protect their Personal Information in violation of the law and in breach of their duties to Class members to keep this information secure.

38. Defendants knew, or should have known, that Excells' system was not secure, that appropriate security systems and technologies were not in place, and that the Personal Information of Plaintiff and Class members' was vulnerable to theft.

39. Excellus knowingly, recklessly, and/or with gross negligence, failed to take reasonable measures to secure its network and protect the Personal Information of Plaintiff and Class members.

40. Indeed, it took Excellus more than 20 months before it even detected the breach to its system. Had Excellus' taken reasonable steps to protect and maintain the security of its system, it would have quickly detected the intrusion and been alerted to the breach.

41. Because Defendants failed to secure the Personal Information of Plaintiff and Class members, this information was unlawfully disclosed to thieves.

42. Plaintiff and other Class members reasonably believed that Defendants employed adequate data security practices and policies. In addition to Defendants' affirmative statements regarding safeguarding customer information, Defendants failed to disclose their negligent and insufficient data security practices and, as a result, Plaintiff and other Class members decided to entrust their information to Defendants, which they would not have done had they known that, in fact, Defendants did not take all necessary precautions to secure their Personal Information. Defendants accepted Class members' Personal Information and fees, but failed to live up to their promises to secure Class members' Personal Information, breaching an implied contract with Plaintiff and Class members.

43. It was not until October or November, that Plaintiff received a letter from Defendants alerting her of the Data Breach and that her Personal Information had been compromised.

44. Consumer's Personal Information is valuable. Indeed, "PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets." John T. Soma, *et al., Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets,* 15 RICH. J.L. & TECH. 11, at *3-4 (2009) (citations omitted). Personal Information is particularly valuable to identity thieves who often trade it on the "cyber black-market" for years. Plaintiff and other Class members have been deprived of the control over and value of their Personal Information, for which there is a well-established market.

45. Because Plaintiff's and Class members' Personal Information has been exposed to thieves, they face a serious and immediate threat of identity theft, fraud, drained bank accounts, phishing, and opening or re-opening of accounts in their name. Fraudulent use of the information can continue for years.

46. The various risks associated with stolen Personal Information have been widely publicized. Defendants knew or should have known about the risk of security breaches and should have taken appropriate and standard measures to guard against such attacks.

47. The Notification Letter advised Plaintiff that Defendants have arranged for her to receive two years of identity theft protection services through Kroll and credit monitoring by TransUnion.

48. The identity theft and credit monitoring services being offered are not adequate in time or comprehensive enough in coverage. At best, the credit monitoring service offered by Defendants may reveal new credit accounts opened with compromised information, but it does nothing to prevent unauthorized charges made to existing accounts.

49. Indeed, Defendants put the burden on Plaintiff and Class members to protect themselves and mitigate their damages – such as placing and removing security freezes on their credit reports, monitoring their credit reports, reviewing their account statements, and changing their passwords. Many mitigation attempts will require Plaintiff and Class members to incur additional out-of-pocket expenses. For example, there are fees required to place and remove a "security freeze" on one's credit report each time it is placed at each of the three credit reporting agencies (Experian, Equifax, and Trans Union). Periodically monitoring one's credit reports would cause a Data Breach victim to incur an expense to see his or her credit reports beyond the one free annual report to which they are entitled.

CLASS ACTION ALLEGATIONS

50. Plaintiff seeks to represent a class defined as all persons in the United States whose Personal Information was accessed as a result of the Data Breach (the "Class").

51. Plaintiff also seeks to represent a subclass defined as all members of the Class who reside in New York (the "New York Subclass").

52. Members of the Class and the New York Subclass are so numerous that their individual joinder herein is impracticable. On information and belief, members of the Class and the New York Subclass number in the millions. The precise number of Class members and their identities are unknown to Plaintiff at this time but may be determined through discovery. Class members may be notified of the pendency of this action by mail and/or publication through the records of Defendants.

53. Common questions of law and fact exist as to all members of the Class and the New York Subclass and predominate over questions affecting only individual Class and New York Subclass members. Common legal and factual questions include, but are not limited to:

a. Whether Defendants engaged in the wrongful conduct alleged herein;

b. Whether Defendants unlawfully disclosed Plaintiff's and Class members' Personal Information;

c. Whether Defendants failed to implement and maintain reasonable security practices and procedures to protect the Personal Information from disclosure;

d. Whether Defendants unreasonably delayed in discovering and/or notifying affected customers of the Data Breach;

e. Whether the Notification Letter provided adequate notice of the Data Breach;

f. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Personal Information they store and which was compromised in the Data Breach;

g. Whether Defendants' conduct was negligent;

h. Whether Defendants entered into and breached an implied contract with Plaintiff and Class members to safeguard their Personal Information;

i. Whether Defendants were unjustly enriched;

j. Whether Defendants violated HIPAA;

k. Whether Defendants violated New York General Business Law § 349; and

l. Whether Plaintiff and the Class are entitled to damages, injunctive relief, restitution or other equitable relief and/or other relief as may be proper.

54. The claims of the named Plaintiff are typical of the claims of the Class and the New York Subclass in that all members of the Class have been subject to and affected by the same conduct and omissions by Defendants. The claims alleged herein are based on the same violations by Defendants that harmed Plaintiff and members of the Class. As victims of the

Data Breach, all members of the Class were subjected to the same wrongful conduct. Plaintiff's claims are typical of the Class' claims and do not conflict with the interests of any other members of the Class. Defendants' unlawful, unfair, deceptive, and/or negligent actions and omissions concern the same business practices described herein irrespective of where they occurred or were experienced.

55. Plaintiff is an adequate representative of the Class and the New York Subclass because her interests do not conflict with the interests of the Class or New York Subclass members she seeks to represent, she has retained competent counsel experienced in prosecuting class actions, and she intends to prosecute this action vigorously. The interests of Class and New York Subclass members will be fairly and adequately protected by Plaintiff and her counsel.

56. The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of Class and New York Subclass members. Each individual member of the Class and New York Subclass may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

COUNT I
Negligence

57. Plaintiff repeats the allegations in the foregoing paragraphs as if fully set forth herein.

58. Plaintiff brings this claim individually and on behalf of the members of the Class and the New York Subclass against Defendants.

59. Defendants came into possession, custody and/or control of confidential Personal Information of Plaintiff and Class members.

60. In collecting the Personal Information of Class members, Defendants owed Plaintiff and the members of the Class a duty to exercise reasonable care in safeguarding, keeping private, and protecting such information from being accessed by and disclosed to third parties. Defendants had a duty to, among other things, maintain and test its security systems and take other reasonable security measures to protect and adequately secure the Personal Information of Plaintiffs and the Class from unauthorized access and use, to implement processes that would detect a breach of security in a timely manner, and to timely disclose to Plaintiff and Class members that their Personal Information had been compromised.

61. Moreover, Defendants had a duty to safeguard the Personal Information of its customers under HIPAA.

62. Defendants were aware that by storing the Personal Information of Class members, they had a responsibility to take reasonable security measures to protect the data from being stolen and accessed.

63. Defendants violated these standards and duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members Personal Information by

failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, and software and hardware systems to safeguard and protect the Personal Information entrusted to them.

64. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' Personal Information would result in the unauthorized release, disclosure, and dissemination to the world of Plaintiff's and Class members' Personal Information for no lawful purpose.

65. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiff and the Class by failing to exercise reasonable care in safeguarding and protecting Class members' Personal Information.

66. Defendants, through their actions and/or omissions, also unlawfully breached their duties to Plaintiff and the Class by failing to timely detect the Data Breach and timely disclose that the Personal Information within Defendants' possession had been released to unauthorized persons.

67. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and continuing increased risk of identity theft and fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) invasion of privacy; (iii) breach of the confidentiality of their Personal Information; (iv) deprivation of the value of their Personal Information, for which there is a well-established market; and/or (v) the

financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

COUNT II
Negligence Per Se

68. Plaintiff repeats the allegations in the foregoing paragraphs as if fully set forth herein.

69. Plaintiff brings this claim individually and on behalf of the members of the Class and the New York Subclass against Defendants.

70. Pursuant to HIPAA, Defendants had a duty to safeguard the Personal Information of Plaintiff and Class members.

71. Defendants violated HIPAA by failing to keep and protect Plaintiff's and Class members' Personal Information and failing to comply with the standards set forth in HIPAA.

72. Defendants' failure to comply with HIPAA and other industry standards and regulations constitutes negligence per se.

COUNT III
Breach of Implied Contract

73. Plaintiff repeats the allegations in the foregoing paragraphs as if fully set forth herein.

74. Plaintiff brings this claim individually and on behalf of the members of the Class and the New York Subclass against Defendants.

75. The Personal Information of Plaintiff and Class members was provided to Excellus in exchange for healthcare services provided by Excellus. Implicit in this transaction was a contract whereby Defendants became obligated to reasonably safeguard Plaintiff's and Class members' Personal Information and promptly notify customers in the even that this information was compromised.

76. Defendants breached the implied contract with Plaintiff and Class members by failing to take reasonable measures to safeguard their Personal Information. Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft and fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their Personal Information; (iv) deprivation of the control over and value of their Personal Information, for which there is a well-established market, and/or (v) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

COUNT IV
Bailment

77. Plaintiff repeats the allegations in the foregoing paragraphs as if fully set forth herein.

78. Plaintiff brings this claim individually and on behalf of the members of the Class and the New York Subclass against Defendants.

79. Plaintiff and other Class members delivered and entrusted their Personal Information to Defendants for the sole purpose of obtaining healthcare services.

80. During the time of bailment, Defendants owed Plaintiff and other Class members a duty to safeguard their Personal Information stored by Defendants by maintaining reasonable security procedures and practices to protect such information. Defendants breached this duty as described herein.

81. As a result of Defendants' breach, Plaintiff and other Class members have been harmed as alleged herein.

COUNT V
Conversion

82. Plaintiff repeats the allegations in the foregoing paragraphs as if fully set forth herein.

83. Plaintiff brings this claim individually and on behalf of the members of the Class and the New York Subclass against Defendants.

84. Plaintiff and Class members were the owners of their Personal Information. As a result of Defendants' wrongful conduct as described herein, Defendants have interfered with Plaintiff's and Class members' right to possess and control their Personal Information, to which they had a superior right of possession and control at the time of the conversion by the Data Breach.

85. Plaintiff and Class members did not consent to Defendants' mishandling and loss of their Personal Information.

86. As a result of the conduct described herein, Plaintiff and the Class suffered injury, damage, loss or harm, and as a result, seek compensatory damages. In acting with malice and in conscious disregard of Plaintiff's and Class members' rights, Plaintiff also seeks and award of punitive damages on behalf of the Class.

COUNT VI
Deceptive Acts or Practices, New York Gen. Bus. Law § 349

87. Plaintiff repeats the allegations in the foregoing paragraphs as if fully set forth herein.

88. Plaintiff brings this claim individually and on behalf of the members of the New York Subclass against Defendants.

89. By the acts and conduct alleged herein, including permitting the Personal Information of Plaintiff and Class members to be exposed through lack of reasonable safeguards, and failing to timely detect and disclose the Data Breach, Defendants committed unfair or deceptive acts and practices in the conduct of their business, trade and commerce in the furnishing of services in this State.

90. The foregoing deceptive acts and practices were directed at consumers.

91. Defendants' practice and course of conduct was likely to mislead, and did mislead, consumers acting reasonably under the circumstances.

92. As a direct and proximate result of Defendants' actions, inaction, and omissions as alleged herein, Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft and fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their Personal Information; (iv) deprivation of the control over and value of their Personal Information, for which there is a well-established market, and/or (v) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

93. On behalf of herself and other members of the New York Subclass, Plaintiff seeks to enjoin the unlawful acts and practices described herein, to recover her actual damages or fifty dollars, whichever is greater, three times actual damages, and reasonable attorneys' fees.

COUNT VII
Unjust Enrichment

94. Plaintiff repeats the allegations in the foregoing paragraphs as if fully set forth herein.

95. Plaintiff brings this claim individually and on behalf of the members of the Class and the New York Subclass against Defendants.

96. Plaintiff and members of the Class conferred benefits on Defendants by paying for healthcare services.

97. Defendants have been unjustly enriched by accepting monetary benefits derived from the healthcare services provided to Plaintiff and Class members. Retention of those moneys under these circumstances is unjust and inequitable because Defendants breached their duties and violated the law by their failure to safeguard Plaintiff's and Class members' Personal Information.

98. Because Defendants' retention of the non-gratuitous benefits conferred on them by Plaintiff and members of the Class is unjust and inequitable, Defendants must pay restitution to Plaintiff and members of the Class for their unjust enrichment, as ordered by the Court.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks a judgment against Defendants, as follows:

A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and New York Subclass and Plaintiff's attorneys as Class Counsel to represent the Class and New York Subclass;

B. For an order declaring that Defendants' conduct violates the statutes referenced herein;

C. For an order finding in favor of Plaintiff and the Class and New York Subclass on all counts asserted herein;

D. For compensatory, statutory, and punitive damages in amounts to be determined by the Court and/or jury;

E. For prejudgment interest on all amounts awarded;

F. For an order of restitution and all other forms of equitable monetary relief;

G. For an order enjoining Defendants from continuing the unlawful practices detailed herein; and

H. For an order awarding Plaintiff and the Class and New York Subclass their reasonable attorneys' fees and expenses and costs of suit.

JURY DEMAND

Plaintiff demands a trial by jury on all causes of action and issues so triable.

Dated: December 10, 2015

Respectfully submitted,

DOLCE PANEPINTO

By: *s/ John Licata*
John Licata
1260 Delaware Avenue
Buffalo, New York 14209
Telephone: (716) 852-1888
Email: jlicata@dolcepanepinto.com

LEVI & KORSINSKY LLP
Shannon L. Hopkins
Shane Rowley
Nancy Kulesa
Andrea Clisura
30 Broad Street, 24th Floor
New York, New York 10004
Telephone: (212) 363-7500
Facsimile: (866) 367-6510
Email: shopkins@zlk.com

srowley@zlk.com
nkulesa@zlk.com
aclisura@zlk.com

Attorneys for Plaintiff